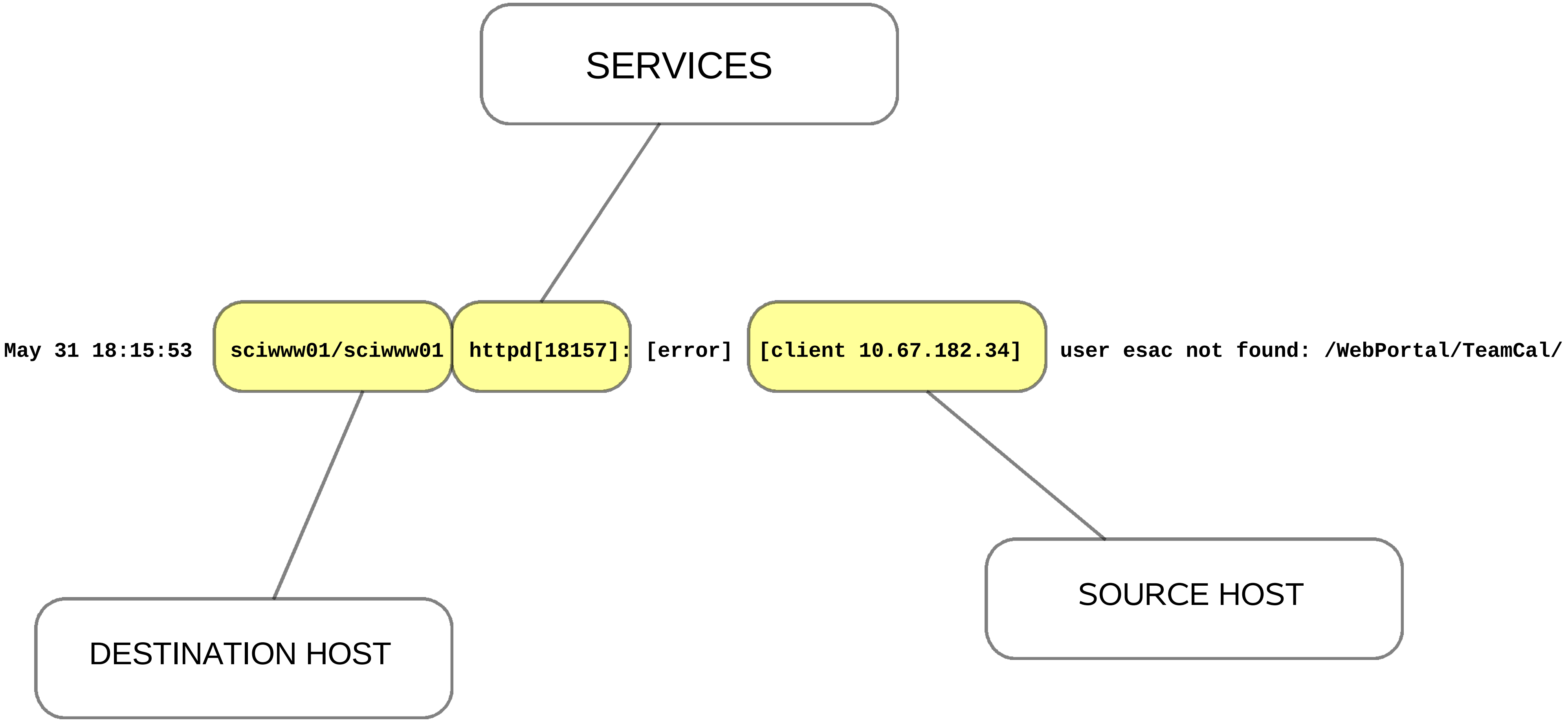
# ESAC Trainee Project

**Adolfo Vazquez, UCM**

## Security Scripts for the Computer Support Group

**Tutor. Ruben Alvarez (CSG)**

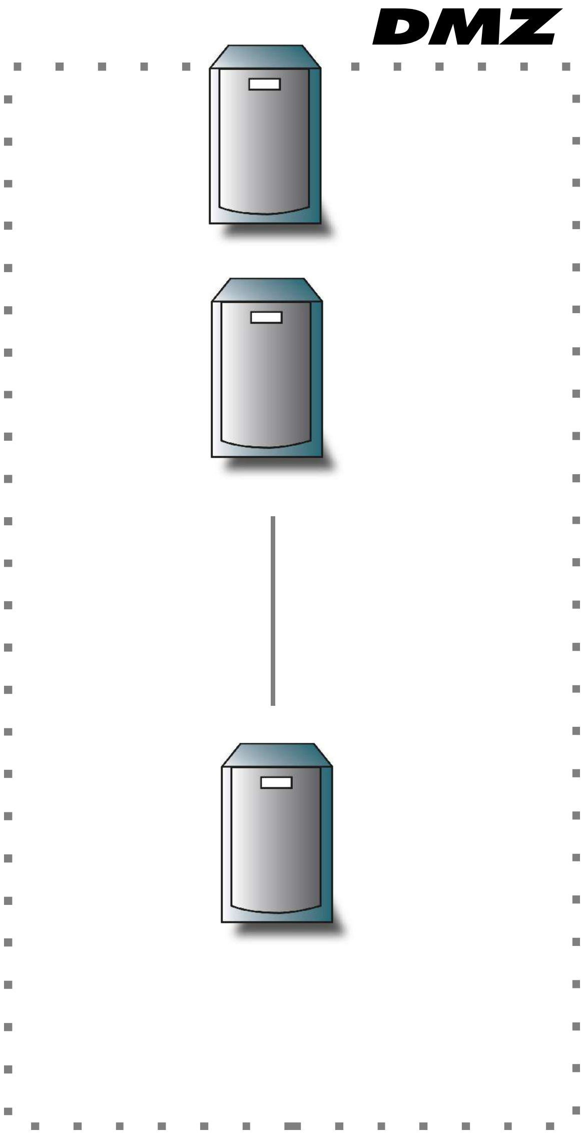


SERVICES

```
May 31 18:15:53  sciwww01/sciwww01  httpd[18157]: [error]  [client 10.67.182.34]  user esac not found: /WebPortal/TeamCal/
```

DESTINATION HOST

SOURCE HOST



CURRENTLY. ~ 50 SERVERS
FUTURE. +100 SERVERS

**LOG ANALYSIS**

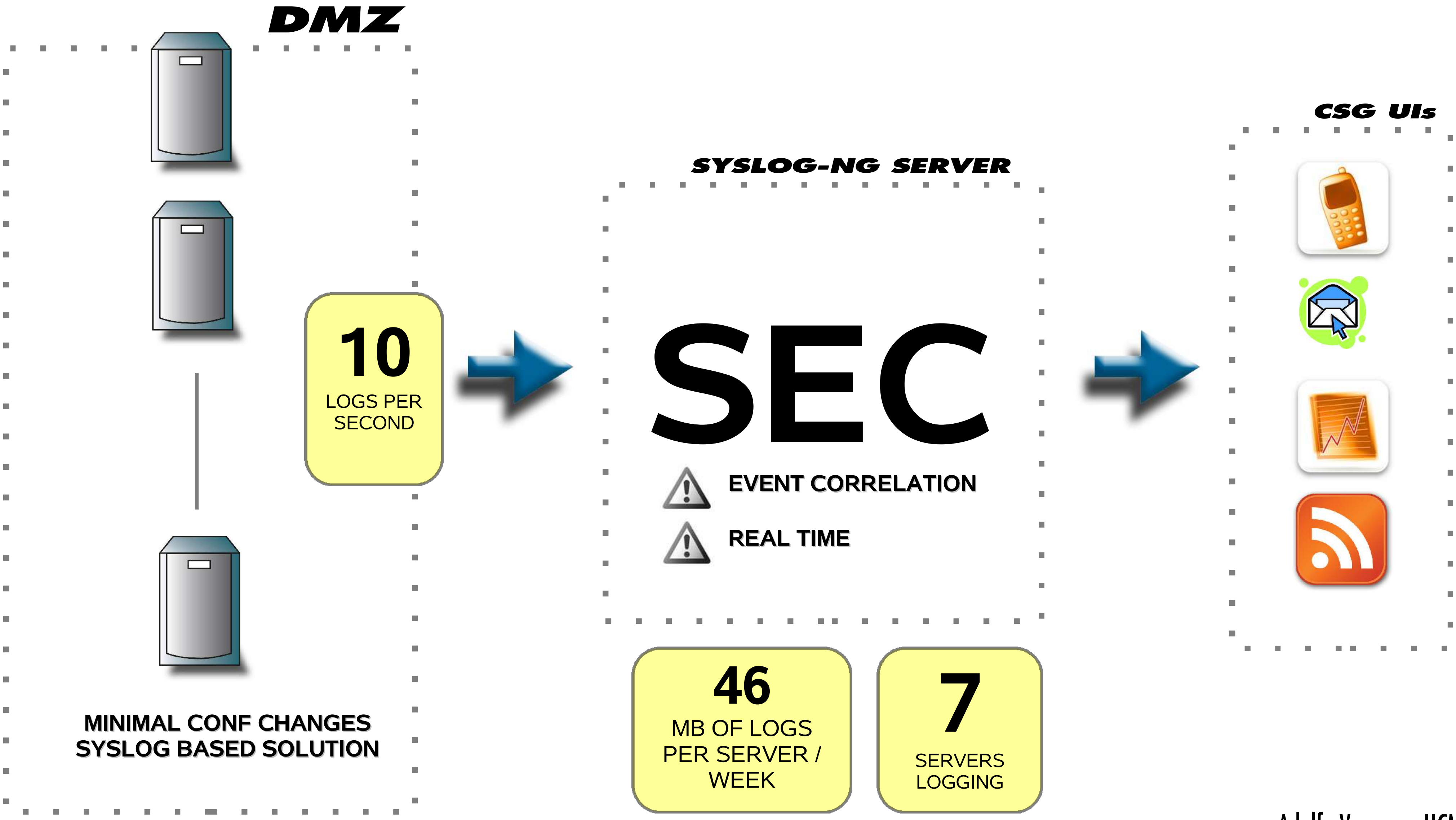
**DIFF**

**FIREWALL!**

## ESAC CASE OF STUDY

# ESAC Trainee Project

esa



DMZ

10

LOGS PER SECOND

MINIMAL CONF CHANGES
SYSLOG BASED SOLUTION

SYSLOG-NG SERVER

SEC

⚠ EVENT CORRELATION

⚠ REAL TIME

46

MB OF LOGS PER SERVER / WEEK

7

SERVERS LOGGING

CSG UIs

## ARCHITECTURE OF PROPOSED SOLUTION

Adolfo Vazquez, UCM
Security Scripts for the Computer Support Group
Tutor. Ruben Alvarez (CSG)

### SYSLOG SERVER

SEC

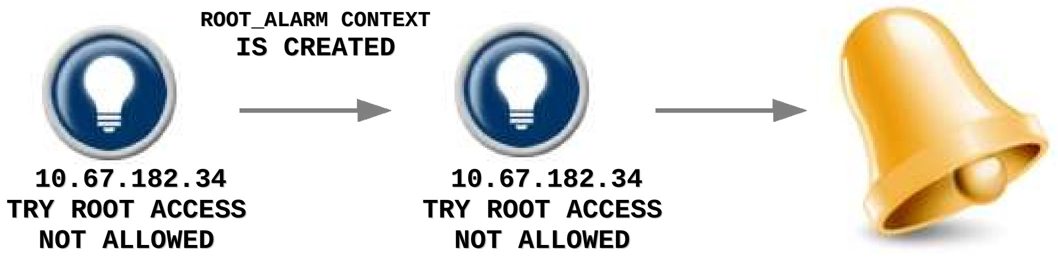
### SEC FEATURES

- Same service on the same machine (root access)
- Several services on the same machine (security scanners)
- Several machines on the same or different services (Denial of Service)

### SEC RULE EXAMPLE

```
type=Single
ptype=SubStr
pattern=sciwww02
action=shellcmd echo llegando
```

### CONTEXTS: SEC MAIN NEW CONCEPT


ROOT_ALARM CONTEXT
IS CREATED

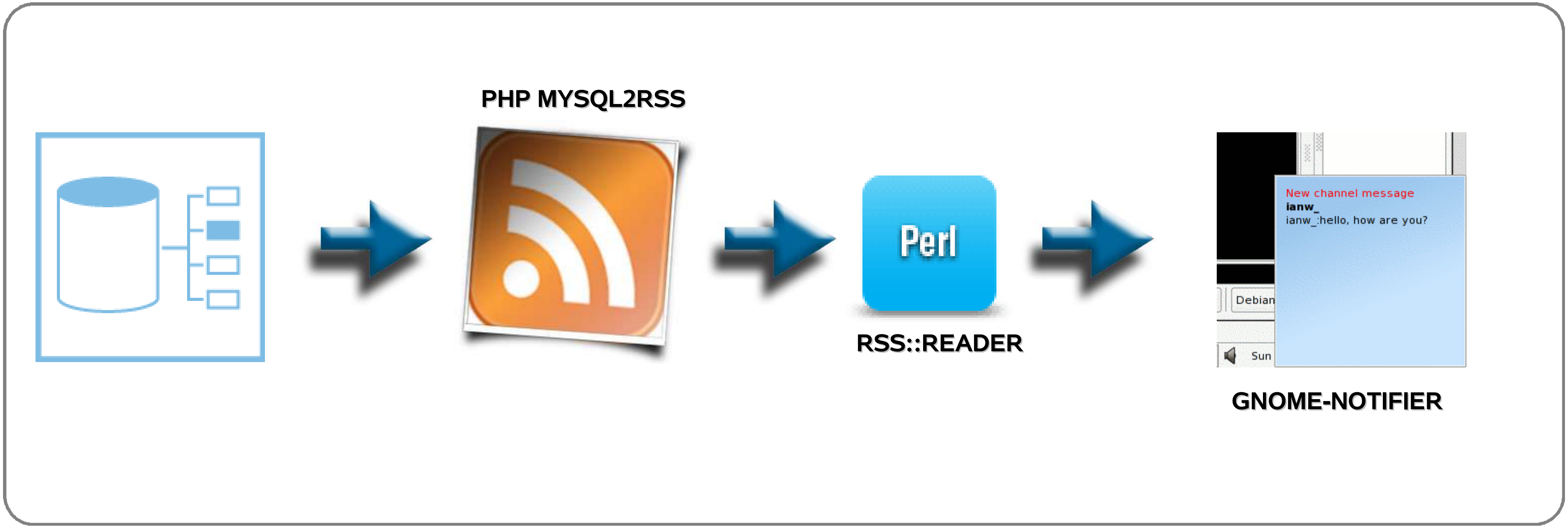
10.67.182.34
TRY ROOT ACCESS
NOT ALLOWED

10.67.182.34
TRY ROOT ACCESS
NOT ALLOWED

Adolfo Vazquez, UCM
Security Scripts for the Computer Support Group
Tutor. Ruben Alvarez (CSG)

SIMPLE EVENT CORRELATION

## POP-UP UI



PHP MYSQL2RSS

RSS::READER

GNOME-NOTIFIER

New channel message
**ianw_**
ianw_:hello, how are you?

## USER INTERFACES

## THE OLD DAYS...

Bryan Sullivan (left) checking spacecraft command data received via a teletype tape from mission control while Ron Hicks makes entries in the computer log book during the Apollo 7 mission